CHAPTER 1.7

Building Trust: The Role of Regulation in Unlocking the Value of Big Data

SCOTT BEARDSLEY
LUIS ENRIQUEZ
FERRY GRIJPINK
SERGIO SANDOVAL
STEVEN SPITTAELS
MALIN STRANDELL-JANSSON
McKinsey & Company

"Data is a precious thing. . ." and "…that's why I've called data the new oil. Because it's a fuel for innovation, powering and energizing our economy."[1] These were the words of Neelie Kroes, Vice-President of the European Commission responsible for the Digital Agenda, when speaking about the value of big data earlier in 2013. As Kroes noted, data comprise a fuel we have only just begun to tap.

This "new oil" is certainly plentiful. Trillions of bytes of data are generated by companies that capture information about their customers, suppliers, and operations. Networked sensors and software embedded in devices and appliances are further energy generators, as are the growing volumes of media content. These sources of data do not even include the billions of individuals around the world generating the same fuel on their smartphones, personal computers, and laptops. And the volumes of data are exploding. McKinsey recently estimated that the data collected globally will grow from some 2,700 exabytes in 2012 to 40,000 exabytes by 2020.[2] To put this into context, a single exabyte of data equals a hundred thousand times all the printed material of the Library of Congress.

Definitions of big data vary greatly. Rather than put a number on what qualifies as "big," McKinsey defines it as datasets so large that typical database software tools are unable to capture, store, manage, and analyze them. Such a definition allows for the fact that the size of datasets regarded as "big" will also grow with the advance of technology.[3]

Whatever the precise definition, big data is widely acknowledged to create value in four ways. It creates greater transparency by making more and better information available more quickly. It helps organizations create highly specific segmentations, enabling them to tailor products and services more precisely. It helps improve decision-making by providing better tools for analysis. And it supports innovation in the form of new products and services.

Big data can create significant value for the whole economy. McKinsey research shows that companies that use big data can deliver productivity and profit gains that are 5 to 6 percent higher than those of competitors. The private sector is not the only beneficiary, however. Big data can also enhance productivity and effectiveness of the public sector and create economic surplus for consumers. For example, the McKinsey Global Institute estimates that US healthcare expenditure could be reduced by 8 percent by using big data to drive efficiency and quality.

No wonder, then, that governments and political institutions are promoting big data on their agendas and adopting initiatives such as the European Union's open data directive, which aims to give both citizens and member governments access to a raft of government

Please note: The views expressed in this article are those of the authors and do not necessarily represent those of McKinsey and Company.

Figure 1: Consumers' privacy protection concerns

Sources: USC Dornslife/Los Angeles Times 2012; European Commission 2011.
* These data are taken from the Special Eurobarometer poll published in 2011. Respondents were asked to select 4 out of 12 possible responses to the question of what should happen to companies that breach protection rules. We present the top 3 responses here.

data. Governments understand that big data's economic and social potential can grow only alongside continued innovation in the underlying technologies, platforms, and analytic capabilities for handling data, as well as the evolution of behavior among its users. Recent McKinsey research shows that enabling "open data" or "liquid data" across seven domains—education, transportation, consumer products, electricity, oil and gas, healthcare, and consumer finance—can generate more than US$3 trillion in additional value a year.[4]

There is no guarantee, however, that this potential will be fully realized. Several obstacles lie in the way. The uptake of big data will depend on the adoption of next-generation telecommunications infrastructure, which is still in its early development in many parts of the world. Another prerequisite is a large enough pool of talent with the advanced analytical skills needed to put the data to good use. This workforce will need to be trained. Equally, big data uptake will hinge on whether ways can be found to protect information technology infrastructures and the data they carry from cyberattacks. A further imperative is to build the trust of citizens, who are growing increasingly suspicious about how information about them is being used.

Regulation plays a role in tackling all these obstacles. This chapter focuses only on the need to build trust. It examines the various broad types of regulatory frameworks that are emerging to protect privacy. Furthermore, it identifies the key issues that regulators will need to consider as their policies evolve if their aim is to foster trust while not stifling the enormous potential of big data, and it outlines some actions companies can take themselves to promote consumer trust.

CONSUMER TRUST AS AN ENABLER OF BIG DATA

Research reveals that consumers are increasingly concerned about how their personal data are used (Figure 1), although the level of concern varies according to the type of data being considered. Consumers care more about their financial transactions and health-related information than about their online habits, for example. The recent revelations by Edward Snowden disclosing US government data collection practices and the extraction of data from a number of large Internet companies have further raised public awareness about privacy issues and data protection in the online world.

If big data is to deliver on its promise, companies will need both to create customer trust in big data applications and their use and to help customers feel safe about the protection of their personal data and privacy. Governments and regulators will need to frame data protection policies that safeguard the privacy of both customers and citizens. At the same time, these policies must not stifle the innovation that big data can deliver, or its attendant economic and social benefits.

DATA PROTECTION ARCHETYPES ACROSS THE WORLD

The protection of personal data has long been viewed as a fundamental right, enabling individuals to be in control of data about their own person and preventing unnecessary listings and discriminatory behavior. Individuals can exercise this control by explicitly giving or withholding consent before their personal data are

used. They have a right to be informed if those data are to be used, and for what purpose. Companies and organizations using their data are also required to protect it from unauthorized use. There are strict measures in place to protect medical data and credit information.

But the issue has become more complicated in the Internet era. Some argue that this right should be safeguarded more strongly than ever when so many companies and organizations are seeking access to personal data and can gain that access more easily. On the other hand, as we have seen, economic, social, and personal benefits can arise from sharing data, and many consumers are perfectly happy to give up some of their privacy in return for certain goods or services.

Data protection laws are evolving not only in an attempt to keep pace with technological developments and new ways of using, collecting, and sharing personal data, but also to keep pace with attitudes toward privacy. To better understand the state of play, McKinsey has conducted extensive research into the data protection regulatory frameworks of more than 20 countries worldwide, identifying the key principles and requirements (Figure 2).

From our research we have identified three main archetypes of the level of regulation imposed around the world: from the least to the most extensive, these are regulations with a light touch, those with a minimum standard, and those with strict ex-ante requirements.

- **Light touch/self-regulation.** This is the approach used in the United States, where there is no general federal data protection law. Instead, different sectors—such as healthcare, telecommunications, and finance—are regulated by specific laws applying only to these sectors. These laws are enforced by sector-specific authorities. Separate states can also stipulate their own general regulations. Generally the onus is on industries and the companies within them to build trust with their customers, either by issuing and following codes of conduct or via contractual arrangements. Companies are responsible for the privacy statements issued to their customers and can face judicial sanctions for non-compliance. Facebook and Google are two recent cases in point.[5]

- **Minimum standard setting.** In Asia, the Asia-Pacific Economic Cooperation (APEC, a forum of 21 Asia-Pacific economies) has developed a self-regulatory framework setting out the principles that economies should implement and companies then follow to ensure a common, minimum level of data protection across member economies. The aim is to enable the easier transfer of data among economies where the level of data protection regulation varies greatly. Although some Asian economies (such as Pakistan) still lack data protection laws entirely or have recently introduced them (e.g., China and India), others—such as Japan—have well-developed laws. Examples of minimum-level principles are the requirement that individuals (where appropriate) should be able to exercise choice about the collection, use, or disclosure of their data, and that the data collected should be accurate, complete, and up to date.[6]

- **Strict ex-ante requirements.** Ex-ante requirements apply in Europe, where both the Council of Europe and the EU Commission have developed extensive frameworks to protect data and privacy in their respective member countries.[7] These frameworks not only define what is regarded as personal data and how such data can and cannot be used, but they also set organizational and technological requirements. Companies should, for example, implement technological and organizational measures to protect the data gathered. Furthermore, strict liabilities are in place relating to both companies and cooperation frameworks for regulators. The frameworks stipulate that data from the European Union may be transferred only to countries that have an appropriate level of protection.[8]

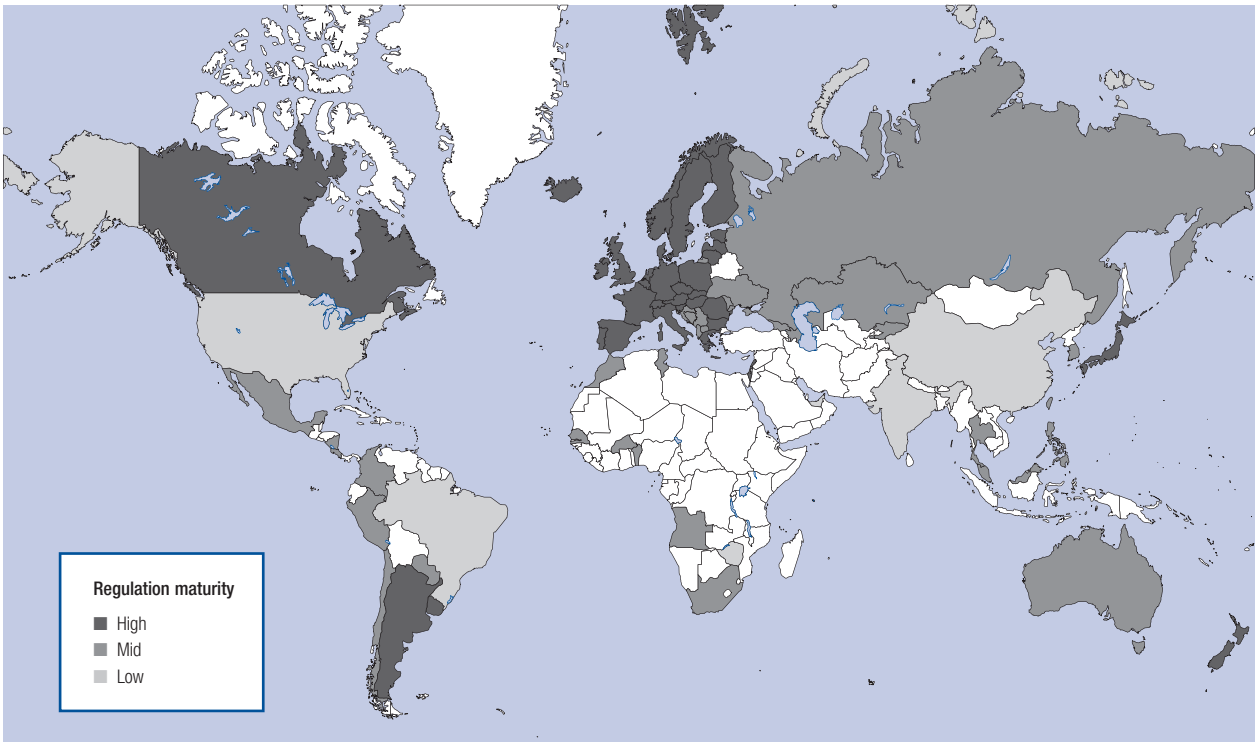
All three regulatory archetypes are constantly evolving. One example of this evolution is that the European Union is currently updating the existing data protection directive from 1995 to better meet the requirements of today's data-intensive world.[9] In the United States, the Federal Trade Commission (FTC) has increased its focus on data protection issues and has published several reports and recommendations on the topic in the past few years. It has also taken on a stricter role regarding the enforcement of companies' own privacy statements.[10] The APEC framework was set up in 2004 and has evolved over the past 10 years.

Opinions on the best approach to data protection and privacy regulation differ. Some experts argue that it is better to adopt a light-touch approach in a technologically dynamic world because detailed, specific regulation could quickly become obsolete and even hinder technological and business development. Others argue that increasingly powerful technology makes a stricter regulatory approach necessary to protect privacy. Whatever approach is taken, we believe data protection and privacy regulation is becoming more and more important across the world, and countries and companies need to embrace it to create competitive advantages for them in the future.

KEY REGULATORY AREAS FOR BIG DATA UPTAKE

Whatever approach any single government or regulator chooses to adopt, all will need to pay particular attention to key areas that require further clarification to support the kind of innovation and prosperity that big

Figure 2: Variation in data protection regulation across markets



UNITED STATES

No federal law exists to date

Some state- and sector-specific laws have stricter regulations

Case-by-case enforcement of privacy statements

SOUTH AMERICA

Tradition of "habeas data"—the right to find out if personal data is processed and the right to file a complaint if it is misused

After amendments, regulation in Argentina and Uruguay is at the EU level of strictness

No specific data protection law exists in Brazil, but the country has constitutional protection and sector-specific data protection legal provisions

EUROPEAN UNION

Existing regulation is already the strictest globally

Regulations cover all industry sectors

Regulation requires "adequate protection"—that is, the same level of protection for transmission to third countries

A safe harbor agreement with the United States enables free data transfer between compliant companies in the two regions

RUSSIA AND CENTRAL ASIA

Data Protection Acts exist in some countries (Azerbaijan, Georgia, Russia, Ukraine)

Enforcement is low (relevant mechanisms and authorities are not always in place)

MIDDLE EAST AND AFRICA

A few countries (Morocco, Tunisia, the United Arab Emirates) already have data protection laws

Morocco signed the Council of Europe data protection convention in 2013,* establishing a general data protection regime

Most countries are unregulated or have single points in sector laws (e.g., Algeria, Egypt)

ASIA PACIFIC

The level of protection ranges from strong protection in Japan and the Republic of Korea to weaker protection in Bangladesh, China, Pakistan, Indonesia, for example

Recent awareness of data protection issues has resulted in several new laws in economies such as India, Hong Kong SAR, the Republic of Korea, and Singapore, as well as other efforts, such as the APEC Cross-Border Privacy Rules System, enhancing protection

Sources: Council of Europe 2013a, b; European Commission 1995, 2002, 2012; IAPP 2013a, b.

* The convention was initiated and signed by Member States of the Council of Europe in 1981. See Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), available at http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.

data can drive, while maintaining customer trust and data protection. These areas include: consent before collection, a definition of *personal data,* anonymization, the right to be forgotten, relevant jurisdiction, and liability issues. Each of these key areas is discussed below.

Consent before data collection. A key principle in the European regulatory framework is the need to obtain personal consent before data are gathered. Anyone wanting to use an individual's data must first seek his or her permission. But with so much information now available and being gathered, seeking that approval can be a slow, tedious process for companies and consumers alike and can hinder big data development. Cookies on the Internet are a simple example. Surfing the web would be more convenient without cookie notifications and approvals. The APEC framework recognizes this, and the framework states that "where appropriate, individuals should be provided with . . . mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information."[11] However, determining where such choice is appropriate is open to interpretation.

The definition of personal data. The suggested EU framework defines *personal data* as "any data that can be attributed to an identifiable person either directly or indirectly." The APEC framework describes *personal data* as "information about an identified or *identifiable* individual." Both these definitions mean that not only data clearly identifying a person with information such as a name or address is considered to be personal data, but also data that can be attributed to a person indirectly through some other measure, such as via a mobile phone number or an identity code. In a big data world where a lot of data are interlinked, it can be difficult to know exactly when data become "personal." Is it only data that identify a person with certainty, or does it also include data that identify someone with high probability? How about a person's actions? Performance? Or buying behavior? To give a concrete example, a US retail chain identified new parents as a very lucrative market segment. The chain analyzed their customers via characteristics such as their shopping habits, age, or marital status to spot customers who were pregnant. They then sent those customers direct marketing material for their baby products ahead of their competitors, who sent their material only after the child's birth.[12] However, information on pregnancies is extremely sensitive, and such material could risk disclosing a pregnancy that has not yet been announced. This could clearly be seen by some as an intrusion of privacy, but the issue is not entirely clear from a legal perspective.

Anonymization. Closely linked to the dilemma of how to define which data are personal is the issue of data anonymization or sanitization. Traditionally, anonymous data have not been subject to data protection laws. However, in a big data world where anonymized data can easily be linked up, it is not very hard to build a profile of a person without traditional means of identification such as a name or address. For example, a team at Harvard was able to identify individuals from anonymized data in a genetics database by cross-referencing it with other public databases. The accuracy rate was 42 percent based on the use of only three types of information—zip code, date of birth, and gender—and rose to 97 percent when the first name or nickname was added.[13] Another example is the use of de-anonymization tools by researchers from Texas University on 500,000 Netflix users who had anonymously voted for their preferred movies back in 2007. In this case, the researchers also managed to identify users by linking the anonymized ratings with another public database with movie ratings.[14] It can therefore be argued that the use of anonymous data can potentially constitute an intrusion of privacy.

Another question related to data anonymization is the right of companies to use the personal data already in their possession and turn them into anonymized data that they sell to others. Some companies are selling their customer data—such as location and application data of telecommunications companies—to other companies in anonymized and aggregated form for marketing purposes. Companies can target their marketing more effectively by using these data to learn about their customers. Internet companies are also matching their customer data and online habits with data from other companies to better target their online advertising.[15] Several questions arise from a privacy perspective. When can data be considered anonymized? Does using a pseudonym make data anonymous? Are companies allowed to use anonymized data without the customer's consent, or must customers give their prior approval? Should that consent be granted before use, or is it enough to allow customers to opt out?

The right to be forgotten. The new EU data protection framework proposes introducing a right for users to request that data controllers remove their personal data from their files. Although on paper it sounds easy to remove personal data relating to an individual upon request, this may not be so easy in the real world. The European Union Agency for Network and Information Security (ENISA) states that a great deal of data are stored in different places in the cloud for security reasons, and these data may have been aggregated or amended into new forms, such as statistical data. Thus removing some specific data from all systems upon request may be entwined with the aggregated data. Clearly this is not such a straightforward task in a virtual environment, and there is no single technical method to enable this easily.[16]

Relevant jurisdiction. Data are increasingly used and stored across borders, but regulation is still largely national in its scope and regulators lack jurisdiction in markets outside their own. The uncertainty about jurisdictions creates problems for companies and

consumers alike. Which regulations apply to companies from another country? Which judicial authority has the right to intervene in disputes? What happens in cases where a company breaches laws across many markets? In its recent proposal on the new EU data protection regulation, the European Union extends the applicability of its regulation to companies outside the European Union that are handling data relating to European Union–based individuals.

Liability issues. In today's world, companies often cooperate to produce big data applications and solutions. One company orders software from another, which in turn uses a third company as a contractor, which stores its data within a cloud service operated by yet another. If data are leaked, it can be very difficult to decide which company is liable.

The above remaining gray areas must be considered and clarified so that both consumers and companies using big data clearly know what the rules are in order to ensure a certain environment that is conducive to investment and market growth. In the next sections we propose several options for regulators and companies to make the big data environment more certain.

IMPLICATIONS FOR REGULATORS AND POLICYMAKERS

Regulators will need to address all the above issues when shaping their personal data protection policies. Although not prescribing any single solution, certain principles will help guide regulators in their deliberations and ensure the necessary regulatory balance. These principles include the need to establish regulatory stability, cooperation with members of industries and different countries, and promoting industry self-regulation. Each of these principles is discussed below.

Regulation in any field always works best if it creates a stable environment in which companies and other organizations can operate. When it comes to data protection, companies and other organizations will need regulatory certainty if innovation is to be encouraged. Providing that stability is likely to be easier if regulators focus not on specific regulations that may quickly become obsolete, but instead on establishing non-discriminatory technology-neutral high-level regulatory principles that last.

Regulators should cooperate with companies and other stakeholders within the industry when revisiting their regulatory frameworks. This will help to understand the business issues and allow them to be at the forefront of developments without hampering industry development.

Regulators should also cooperate internationally to establish common international norms and clarity around applicable legislation. International discussions are already taking place on specific issues. Regulators in the European Union and the United States have a safe harbor framework, for example, that allows US-based companies to transfer data between the two regions without further approval from EU-based regulators. These safe harbor provisions are currently being revisited. US and Asian regulators are cooperating around the APEC framework; the United States is the first non-APEC market to sign the minimum standard framework. An even a wider take on data protection issues in the big data environment would be beneficial for all parties.

Whatever their approach to regulation, governments should promote industry self-regulation. Self-regulation is the best way to achieve a commonly accepted code of conduct for a specific industry. This has already been done in specific areas—for example, the use of personal data in mobile marketing—but so far efforts have occurred mainly at the country level, in markets such as the United States and the United Kingdom. An international industry standard specifically concerning the use of personal data protection in big data would certainly be beneficial to establish a higher level of trust among consumers and create a clear data protection standard for companies. The weakness of industry self-regulation is obviously enforcement, because self-regulation is not normally legally binding.

By efficiently managing all stakeholders, regulators can establish a transparent legal framework that helps promote industry growth rather than hindering it with unnecessary legal burdens.

IMPLICATIONS FOR COMPANIES

The onus is not just on regulators to build an environment of trust where citizens feel their privacy will be properly protected. Companies also have a key role to play. If they develop an efficient data protection strategy, companies may also gain competitive advantage in the form of cost savings, organizational efficiency, and—importantly—reputational advantage. To maximize the benefits of big data and to build trust, a number of actions could be considered.

The first action a company should take is to assess its regulatory and operational starting point. Understanding customer concerns and regulatory issues early will help companies determine the areas of risk they need to start tackling. It will also outline the company's strengths and determine the best way to leverage those strengths to develop their big data strategy. For example, a company may wish to build on its reputation as a reliable company that safeguards customers' personal data or position itself as an innovative company with cool services based on its users' behavior and habits or preferences.

A company should also build a privacy-by-design mentality. It goes without saying that companies will need to comply with relevant regulations. But gaining consumers' trust is a question of mentality, too. Many companies may find they need to implement changes across the organization as well as in relevant processes and technology applications to protect consumer privacy.

Companies should strive to make data protection part of the company culture. They can avoid costs occurring at a later stage (when compliance measures are needed) by implementing data protection in their processes from the start.

Companies must also cooperate with regulatory authorities. Privacy and data protection regulation is constantly evolving. This means that companies will need to establish a close relationship with national regulators to ensure compliance and to make certain that the regulators and policymakers understand the business issues at hand and the benefits of big data for society.

Furthermore, companies need to cooperate with other industry participants. Cooperating to develop industry-specific norms and standards will help to create an industry norm that enables consumers to have greater trust.

Importantly, companies also should empower customers. Customers' concerns about privacy are often alleviated if they are able to make their own decisions about what data they do or do not share. Providing transparent privacy policies or simply informing the customer of the scope of data handling as well as requesting clear consent declarations from customers also helps create customer trust without sacrificing big data business opportunities. Technological tools help, as they can allow customers to adjust their privacy settings and choose whether to opt in or out of services. One example of this is British Telecom's cookie settings, which allow the customer to set the level of cookies allowed and choose the level of privacy they are ready to sacrifice for better services or service quality.

Companies have a key role to play in creating consumer trust. Success in this area is not only about managing regulators and compliance, but also about creating a reputation as trustworthy and reliable in terms of both secure operations and fair commercial practices. As mentioned in the beginning of this chapter, customers are usually willing to share personal data if the value of the service is attractive enough and the customers feel they get more in return than they give up.

CONCLUSION

Big data offers a wide range of opportunities—not just for individual companies, but also for nations and society as a whole. Both regulators and companies have large roles to play to ensure positive development in this emerging market with such great potential.

Regulators and policymakers should respond swiftly to regulatory and policy concerns regarding big data development. They must enable fast network build-out. They must also ensure the education and training of a qualified workforce and safeguard Internet safety. And they must address consumer disquiet about privacy and the protection of personal data—an area where several issues are unclear and require further consideration and clarification, ideally in cooperation with players across the industry value chain and at an international level.

Above, a number of suggestions about how companies might respond to these concerns were outlined. Initially companies should conduct an assessment of their regulatory and operational status quo to identify risks and opportunities. They should consider implementing a privacy-by-design mentality to avoid unnecessary costs while ensuring compliance. Companies should also consider cooperating both with regulators and others within their industry to create trust of their specific sector. Key for gaining customer trust will, however, be the empowerment of customers by clearly communicating their privacy policies to them, giving them options for their privacy settings, and requesting consent declarations. Companies need to ensure that their customers understand what choice means in terms of service performance and make sure their services are providing more value to the customer than the loss of privacy is worth.

It is only by addressing customer concerns at different levels within the industry that the big data industry can eventually evolve to its full potential.

NOTES

1 Kroes 2013a, b.

2 Lund et al. 2013.

3 Manyika et al. 2011.

4 Manyika et al. 2013.

5 FTC 2010–14; see www.ftc.gov/opa/reporter/privacy/privacypromises.shtml.

6 APEC 2005.

7 Council of Europe 1981; European Commission 1995, 2002.

8 European Commission 1995.

9 European Commission 2012.

10 FTC 2010-2014; see www.ftc.gov/opa/reporter/privacy/privacypromises.shtml.

11 APEC 2005.

12 Duhigg 2012.

13 Sweeney et al. 2013.

14 Narayanan and Shmatikov 2008.

15 Steel 2012.

16 ENISA 2011.

REFERENCES

APEC (Asia-Pacific Economic Cooperation). 2005. *APEC Privacy Framework.* Available at http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx.

Beardsley, S., L. Enriquez, W. Torfs, F. Grijpink, S. Newman, S. Sandoval, and M. Strandell-Jansson. 2013. "Re-Establishing the European Union's Competitiveness with the Next Wave of Investment in Telecommunications." In *The Global Information Technology Report: Growth and Jobs in a Hyperconnected World.* Geneva: World Economic Forum, INSEAD, and Cornell University. 93–100.

Council of Europe. 1981. *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.* Available at http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.

———. 2013a. Human Rights and Rule of Law: Data Protection. Available at http://www.coe.int/t/dghl/standardsetting/DataProtection/default_en.asp.

———. 2013b. Human Rights and Rule of Law: Data Protection: National Laws. Available at http://www.coe.int/t/dghl/standardsetting/dataprotection/National%20laws/National_laws_en.asp.

Duhigg, C. 2012. "How Companies Learn Your Secrets." *The New York Times,* February 16. Available at http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all&_r=1&.

ENISA (European Union Agency for Network and Information Society). 2011. *The Right To Be Forgotten: Between Expectations and Practice.* Heraklion, Greece: ENISA. Available at https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten/.

European Commission. 1995. *Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data.* Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

———. 2002. *Directive 2002/58 on Privacy and Electronic Communications.* Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0037:EN:PDF.

———. 2011. *Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union.* Brussels: Directorate-General Communication. Available at http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf.

———. 2012. *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation),* COM (2012) 11 final. Available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

FTC (Federal Trade Commission). 2010–14. *Protecting Consumer Privacy: Making Sure Companies Keep Their Privacy Promises to Consumers.* Available at www.ftc.gov/opa/reporter/privacy/privacypromises.shtml.

IAPP (International Association of Privacy Professionals). 2013a. IAPP Home Page. Available at https://www.privacyassociation.org/.

———. 2013b. IAPP: Data Protection Authorities. Available at https://www.privacyassociation.org/resource_center/data_protection_authorities.

Kroes, N. 2013a. "The Big Data Revolution." Speech given by Neelie Kroes, Vice President of the European Commission responsible for the Digital Agenda, March 26. Available at http://europa.eu/rapid/press-release_SPEECH-13-261_en.htm.

———. 2013b. "The Economic and Social Benefits of Big Data." Speech given by Neelie Kroes, Vice President of the European Commission responsible for the Digital Agenda, May 23. Available at http://europa.eu/rapid/press-release_SPEECH-13-450_en.htm.

Lund, S., J. Manyika, S. Nyquist, L. Mendonca, and S. Ramaswamy. 2013. "Game Changers: Five Opportunities for US Growth and Renewal." *McKinsey Global Institute Report,* July. Available at http://www.mckinsey.com/insights/americas/us_game_changers.

Manyika, J., M. Chui, B. Brown, J. Bughin, R. Dobbs, C. Roxburgh, and A. Hung Byers. 2011. "Big Data: The Next Frontier for Innovation,Competition and Productivity." *McKinsey Global Institute Report,* May. Available at http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation.

Manyika, J., M. Chui, D. Farrell, S. Van Kuiken, P. Groves, and E. Almasi Doshi. 2013. "Open Data: Unlocking Innovation and Performance with Liquid Information." *McKinsey Global Institute, McKinsey Center for Government, and McKinsey Business Technology Office Report,* October. Available at http://www.mckinsey.com/insights/business_technology/open_data_unlocking_innovation_and_performance_with_liquid_information.

Naranyanan, A. and V. Shmatikov. 2008. *Robust De-anonymization of Large Datasets,* February 5. The University of Texas at Austin. Available at http://arxiv.org/PS_cache/cs/pdf/0610/0610105v2.pdf.

Steel, E. 2012."Datalogix Leads Path in Online Tracking." *The Financial Times,* September 23. Available at http://www.ft.com/intl/cms/s/2/8b9faecc-0584-11e2-9ebd-00144feabdc0.html#axzz2idgoMkIT.

Sweeney, L., A. Abu, and J. Winn. 2013. *Identifying Participants in the Personal Genome Project by Name.* Harvard University. Data Privacy Lab. White Paper 1021-1, April 24. Available at http://dataprivacylab.org/projects/pgp/.

USC Dornsife/Los Angeles Times. 2012. "Voters Across the Political Spectrum Concerned About Tech Companies Invading Their Privacy." Press Release, March 21. Available at http://dornsife.usc.edu/usc-lat-poll-privacy-march-2012/.